Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-38. (Canceled)

39. (Currently amended): A digital signing method, comprising:

providing a log list comprising previously generated digital signatures;

computing a hash value of inputted data including a message to be signed or a hash value thereof, the inputted data further including an earlier generated digital signature obtained from the log list or a hash value thereof;

encoding the computed hash value of the inputted data to produce encoded data of a predetermined format that is suitable for encryption processing for generating a signature;

applying a secret key to the encoded data to ~~generate a~~ produce a generated digital signature ~~for the message to be signed~~;

registering as log data ~~including~~ the generated digital signature ~~on a~~in the log list; and

distributing a signature-attached data including the generated digital signature ~~for the message to be signed~~, the message to be signed, and the earlier generated digital signature or the hash value thereof ~~previous log data or the hash value thereof for generating the signature; and~~

~~wherein the inputted data used for generating the digital signature further includes another log data or a hash value thereof that has previously been generated and registered on the log list~~.

40. (Previously presented): The digital signing method of claim 39, wherein said log data further comprises a distribution destination, and wherein said log data including a distribution destination attached thereto.

41. (Previously presented): The digital signing method of claim 39, said method further comprising:

permitting registration of the log data with said log list only when the data from a previously signed message is included in the latest log data registered with said log list.

42. (Previously presented): The digital signing method of claim 39, said method further comprising:

obtaining a timestamp from a trusted authority, said timestamp generated by applying a second secret key to the digital signature, and a time; and

distributing a signature-attached data including the generated digital signature for the message to be signed, the message to be signed, the previous log data or the hash value thereof for generating the signature, and the timestamp.

43. (Currently amended): A digital signing apparatus, comprising:

a processor; and

a storage medium to store a log list comprising previously generated digital signatures, wherein

said processor computes a hash value of inputted data including a message to be signed or a hash value thereof, the inputted data further including an earlier generated digital signature obtained from the log list or a hash value thereof, and wherein

said processor encodes the computed hash value of the inputted data into encoded data of a predetermined format that is suitable for encryption processing for generating a signature;

said processor applies a secret key to the encoded data to ~~generate a~~ produce a generated digital signature~~ for the message to be signed~~;

said processor prepares a signature-attached data including the generated digital signature for the message to be signed, the message to be signed, and the previous log data or the hash value thereof for generating the signature; and said processor registers as log data ~~of said~~the signature-attached data~~ with a~~ in the log list~~ in said storage medium~~.

44. (Previously presented): The digital signing apparatus of claim 43, wherein

said processor applies said secret key to a message or the hash value thereof to generate a digital signature for the message; and wherein

said processor prepares a signature-attached data that includes the generated digital signature, the message, and the previous log data or hash value thereof; and wherein

said processor registers log data of a signature-attached data including the generated digital signature, the message, and the previous log data or hash value thereof, with said log list.

45. (Previously presented): The digital signing apparatus of claim 43, wherein said log data further comprises a distribution destination.

46. (Previously presented): The digital signing apparatus of claim 43, wherein:

registration of the log data with said log list is permitted only when the previous log data is included in the latest log data registered with said log list.

47. (Previously presented): The digital signing apparatus of claim 43, wherein:

said processor obtains a timestamp from a trusted authority, said timestamp generated by applying a second secret key to the digital signature, and a time; and

said processor prepares said signature-attached data including the generated digital signature, the message, and the previous log data or hash value thereof, and the timestamp.

48. (Previously presented): The digital signing apparatus of claim 43, further comprising: an interface configured to be connectable to a computer.

49. (Previously presented): The digital signing apparatus of claim 48, wherein:

if a number of the log data registered with the log list exceeds a particular value, said processor outputs at least one of a plurality of log data registered with the log list to said computer, whereupon said computer registers said at least one of a plurality of log data with a second log list prepared in said computer, and thereupon,

said processor deletes said at least one of a plurality of log data from said log list in said storage medium.

50. (Currently amended): A computer program product for creating a digital signature, said program product comprising:

program code to maintain a log list comprising previously generated digital signatures;

program code to operate a processor to compute a hash value of inputted data including a message to be signed or a hash value thereof, the inputted data further including an earlier generated digital signature obtained from the log list or a hash value thereof;

program code to operate the processor to encode the computed hash value of the inputted data into predetermined format data that is suitable for encryption processing for generating a signature;

program code to operate the processor to apply a secret key to the encoded data to ~~generate a~~ produce a generated digital signature ~~for the message to be signed~~;

program code to operate the processor to register as log data ~~including~~ the generated digital signature ~~on~~ in the ~~a~~ log list ~~in said storage medium~~; and

a computer readable storage medium for embodying the program codes.

51. (Previously presented): A computer program product of claim 50, wherein the computer readable storage medium is a computer readable medium for storing the codes.

52. (Previously presented): A computer program product of claim 50, wherein the computer readable storage medium is a computer readable medium for transmitting the codes.